1-2007

Phishing with a Poisoned Bait

Warren B. CHIK
Singapore Management University, warrenchik@smu.edu.sg

Phishing with a Poisoned Bait

Warren B. Chik

Published in Singapore Law Gazette, 2007 January

This article discusses the problem of dealing with electronic fraud and identity theft under the current Singapore criminal law.

Cybercrime and the Rising Problem of Electronic Fraud and Identity Theft

Computer-related crime consists of two categories of offences: Computer crimes and Cybercrime. 'Computer crime' refers to any criminal activities that are committed *against* a computer or similar device, and data or program therein. In computer crimes, the computer is the *target* of criminal activities. Due to its very nature, computer crimes are generally new, technology-specific criminal behaviour for which specialised legislation is required. In Singapore, the Computer Misuse Act (Cap 50A) ('CMA') was specifically enacted to deal with such problems and the Act has been amended several times since its enactment in 1993 to deal with new forms of offences against the computer.[1] 'Cybercrime' is a general term that refers to offences committed *through* the use of the computer. It is a sub-category of the general term 'crime' and the only difference is that it involves the use of the computer as a *facilitative device* and the use of electronic communications media as a means to commit what are essentially 'traditional' offences such as fraud, cheating and theft. The two categories may overlap and they may both apply to a fact situation, particularly one involving the use or manipulation of a computer and its contents in order to further an offence.[2]

The problem of electronically perpetrated fraud, particularly through theft of virtual identity and security information, is on the rise. There are many scams perpetrated through the use of various forms of information technology. For example, we are all familiar with the Nigerian scam involving advance fee fraud. But the one that has risen in prominence and that is particularly problematic given its insidiously deceptive nature as well as its ability to mutate into more insidious forms in reaction to consumer sophistication, defence technology as well as industry and government controls is what is popularly known as 'phishing'.

Phishing is often not legally defined although the acts involved may be covered under a criminal legal provision; thus, the non-legal definition will be used for our purposes of analysis. In the dictionary, it is defined as 'the practice of luring unsuspecting Internet users to a fake Web site by using authentic-looking email with the real organization's logo, in an attempt to steal passwords, financial or personal information, or introduce a virus attack; the creation of a Web site replica for fooling unsuspecting Internet users into submitting personal or financial information or passwords.'[3] The main elements of phishing or a related activity are as follows:

1 An identity theft through theft of personal identifiable information and/or theft of security information;

2 Carried out through fraud or deception using a fake web site that appears to represent a legitimate entity (essentially another identity theft);

3 Often for ulterior purposes such as to sell the information to other criminal parties or for other criminal uses; or to use it to obtain a transfer of property, most likely financial assets from the victim.

The identity theft can be carried out through several means or techniques including inducing the visitor to the web site, who has a relationship with the real entity, to provide the relevant information; or through the use of malware such as surveillance or stealth technology by causing the visitor to download it onto their computer.

A classic example of phishing involves an identity thief setting up a web site that resembles that of a major bank (often with a deceptively similar domain name). The thief then sends out e-mails en masse claiming to be from that bank requesting the e-mail recipients to input their personal banking information (such as their PIN) into the web site (which hyperlink is provided) so that the bank may update their records or to facilitate a security check. Once the scammer gets hold of the relevant personal information, they will then attempt to access the victim's bank account to transfer the latter's funds to their own accounts and thereafter withdraw the funds before their scam or identity is exposed.

Even as we grapple with the phishing problem, we already see variants of it emerging. New technologies emerge that can be both used and abused, including new forms of information technology such as Instant Messaging ('IM') Systems and VoiP ('vishing') as well as surveillance technology that has led to more innovative crimeware techniques and of 'blended threats' such as 'pharming' and 'spy-phishing' where the hijacking of domain names and the installation of spyware applications are used to aid in cyber fraud and identity theft.

Now that we have identified the acts and motives as well as the parties (in particular the many victims) involved, we can address the adequacy of our current criminal laws in dealing with the various stages of the illegitimate activity.

Such cyber fraud cum identity theft offences that have been described above are on the rise worldwide as shown by many studies conducted.[4] In Singapore as well, there have been more and more reports of such scams involving main banks and other financial institutions. In July 2006 alone, there was a spate of cases reported involving several major banks.[5] Even the Monetary Authority of Singapore, the country's central bank, was a target of a phishing scam.

Does Singapore Criminal Law Adequately Address Phishing or Related Offences?

A phishing or related activity involves various stages of action and players. The preparatory acts and ultimate goals as well as the intentions and motives are equally relevant to the question of whether a punishment for any one stage of the activity should be formulated. The following inquiry into existing

law will largely deal with the adequacy or otherwise of current criminal laws on the presumption that criminalisation and punishment of the action are necessary.

Acts against spoofed targets

A CMA crime may be committed depending on the modus operandi. For instance, if surveillance technology is used to gain unauthorised access to computer material (s 3); to modify computer material (s 5); or if technology is used to use or intercept computer service without proper authority (s 6).[6] However, that is not necessarily the case, for instance, in the conventional case of phishing, which is merely carried out through communications and web-hosting services. There is no offence of personation made out under s 416 of the Penal Code (Cap 224) as it has to involve the impersonation of a real or fictitious 'person', which does not extend to artificial entities or automatic agents. There may also be intellectual property infringement under the Trademarks Act (Cap 332), Copyright Act (Cap 63) and the common law action of passing off. However, the next question is whether the punishment provisions under these offences are adequate to meet the objectives of criminal justice,[7] which in this case, other than upholding the policy objectives of securing computer material against unauthorised access or modification or protecting intellectual property rights, is also justified as a deterrent and preventative measure. Perhaps the Spam Control Bill of 2006 may have some effect if it is enacted into law, but again, the remedies and penalties are inadequate as deterrence to, or to punish, offenders.

Acts against the primary target through theft of ID/security information

In Singapore, there is self-regulation in the private sector for some form of data protection.[8] However, there is no general legal recourse, civil or criminal, for the taking of personal identifiable information per se.[9] Hence, it is fairly accurate to say that there are no general personal informational privacy and data protection laws for the protection of personal information.[10]

However, it is a different thing if the information is used to commit or to further the commission of a 'traditional' offence, which is likely to be the case as phishing and related activities are often motivated by illegitimate pecuniary interests and wrongful financial gain. Section 4 of the CMA may be operative here. However, it is useful only to a limited extent for several reasons inherent to the provision itself. First, under sub-s (1), it requires access, unauthorised or otherwise, to computer material as a prerequisite to an offence made out, which rules out non-computer intrusive methods of fraud and theft. Second, under sub-s (2), it is limited to apply only to access intended for the commission or the facilitation of the commission of an offence involving property, fraud, dishonesty or the causing of bodily harm and which is punishable on conviction with imprisonment for a term of not less than two years. Third, some of these offences, which appear in the Penal Code, either do not appear applicable or are clearly inapplicable to cyber fraud and online property offences such as theft and cheating.[11]

In relation to the third point, for example, under s 415 of the Penal Code, the offence of cheating may apply to acts of phishing with the purpose of using stolen information for unlawful economic gain.[12] However, it clearly does not apply to the offences of theft or criminal misappropriation of property as these offences refer to 'movable property' only.[13] Of course, the same problems of applicability and coverage apply to the criminal provisions, whether under the Penal Code or any other statute as many of

these provisions were drafted before the electronic age and have not been amended since to ensure that certain words and their definition, interpretation or description are rendered applicable to the electronic acts, digital products or to the virtual environment.

Other entities may also be implicated or involve further complicating matters. For example, banks that offer Internet or phone banking may be deceived into transferring a customer's funds to a scammer's account. What are the responsibilities of these entities and did they fulfill them by, for example, the security measures that they have undertaken in relation to such transactions and what are their duties in their relationship with customers particularly if the scammer is not identified, arrested, prosecuted or the assets recovered? These are issues that have to be resolved as they relate to electronic transactions.

To ensure that laws are applicable and effective, we have to enact new laws, either as stand-alone statutes or as provisions under the Penal Code or the CMA to deal with this and other forms of cybercrime, and in a manner that is as technologically and technique-neutral as possible without compromising on civil liberties and the fairness and certainty of the law.

The Problem of Jurisdiction in a Uni-Territorial Cyberspace

Even if substantive criminal laws have been amended in response to the problem specific to electronically-perpetrated fraud and theft, they may have little or no effect if most of such fraud is perpetrated by persons or entities from another country. It has been shown that most of such scams originate in certain countries although they have global reach.[14] Extra-territorial laws such as s 11 of the CMA are required.[15] Even then, the cooperation of other countries is often required in order for a country to obtain evidence (e.g. through mutual legal assistance) jurisdiction over the person (e.g. through extradition) and his assets (e.g. through recognition and enforcement of foreign judgments). In this respect, domestic law reform alone is insufficient and it has to be supported by bilateral, regional and international agreements to reinforce a globally concerted effort to fight what is essentially a common global problem. The Council of Europe's Convention on Cybercrime of 2001, which entered into force on 1 July 2004, is an example of an attempt at a multilateral solution through international fora. Other governmental, private and combined efforts have also been launched in other fora including the G8, United Nations ('UN'), European Union ('EU'), Organization for Economic Cooperation and Development ('OECD'), the Council for Security Cooperation in the Asia Pacific ('CSCAP') and INTERPOL. Perhaps something could be done, at least regionally, within the aegis of ASEAN as well.

CHART (LOOK AT PDF FOR REFERENCE)

Table 1: Stages of a Phishing or Related Offence

Potential Victim

Secondary Target (spoofed entity)

Primary Target (individual user or consumer)

Primary Target (individual user or consumer)

Secondary Target (other entities)

'Property' Stolen through Deception

1 Corporate or public identity (i.e. through acts of forgery)

2 Identity and identifiable information (e.g. passwords, ID, security codes, etc.)

3 Other assets, financial or otherwise, in physical or digital form (e.g. transfer of assets) owned by an individual that may be in the custody or control of another entity

Possible Legal Recourse

* Copyright and Trademark infringement protection laws
* Anti-Spam laws
* Criminal law, if any
* Privacy and data protection laws
* Other laws (e.g. various forms of fraud)
* Criminal law, if any
* Criminal law, if applicable (e.g. existing criminal law such as theft and cheating)

1 Other laws (e.g. various forms of fraud)

Policy Objective of Criminalisation

* The integrity of information technology for interaction and transactions
* Pre-emptive effect (deters and prevents 2 & 3)
* Punitive effect

* Protecting human dignity and personal privacy
* Pre-emptive effect (deters and prevents 3)

* Punitive effect

* Pre-emptive and punitive effect if offence is made out without the offence necessarily carried out (criminalising preparation and intention)
* Punitive effect if offence is required to be made out (criminalising realisation and intention)

Options for Legislation

The following are the options that Singapore can take to update its laws to tackle this problem:

1 Amend the Computer Misuse Act to include provisions on cyber forgery, cyber fraud and identity theft. The effect here will erase the distinction in treatment of computer and cyber crime; however, for practical purposes there is no reason why that distinction has to be maintained in the first place; second, the words 'computer misuse' are wide enough to encompass such offences (although its stated objective may also have to be updated); and third, the extra-territorial provision under the CMA will be applicable and useful to deal with such offences; or

2 Amend the relevant provisions under the Penal Code referable back to s 3 of the CMA.[16] However, this is an indirect measure and may not be adequate; also, the punishment provision under s 3 is arguably inadequate as a deterrence or punishment; and/or

3 Incorporate relevant provisions (particularly relating to identity theft) under new legislation on privacy and data protection for the protection of identifiable personal information. This will require the enactment of such a legislation with its larger objectives in mind, which may take several years to come into fruition; or

4 Amend the Spam Control Bill to incorporate 'spam-plus' provisions relating to spam that is used to perpetrate such offences. The problem with this option is that the coverage is limited to the devices, technology and techniques used to perpetrate spam as defined under the bill which may not take into account newer means and methods of cyber forgery, cyber fraud and identity theft; and also

5 In any event, the punishment provision for these offences should be updated to suit the crime and an extra-territorial provision should be incorporated to ensure effectiveness of coverage.

In order for greater reach of legislation and for effective enforcement, transnational legal and cooperative measures will have to be contemplated. Perhaps Singapore should consider acceding to the Cybercrime Convention that is open to all nations to join. For one, the current computer-related criminal provisions under Singapore law already satisfy most of the substantive requirements under the framework Convention, and investigative powers and procedures can be augmented by legislation, proper training and allocation of resources. The more controversial portion relates to the third main portion of the Convention relating to mutual legal assistance between signatory states and although these provisions will be useful, a more in-depth analysis of the burden on resources and policy concerns will have to be weighed against the benefits of their use before a decision can be made on whether Singapore should join the Convention or not. The other alternative is to include some or all computer-related offences in mutual legal assistance agreements and recognition and enforcement treaties, but it will have

to be a country-to-country piecemeal approach and its effectiveness will be more cumulative than expansive.

Asst Prof Warren Chik
Singapore Management University
E-mail: warrenchik@smu.edu.sg

Notes

1 The Singapore Computer Misuse Act (Cap 50A), which was enacted in 1993, was modelled after the United Kingdom Computer Misuse Act of 1990. Ironically, the Singapore Act is now more updated than the UK Act, which has not been amended since it first came into effect. However, the UK is now considering some amendments to modernise their Act in order to deal with new problems that have arisen since its creation.

2 In fact, there is a provision under the Singapore CMA that makes it an offence to access computer material to commit or to facilitate the commission of an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than two years. See s 4 of the CMA. See also s 10 of the CMA, which makes it an offence to abet, attempt or even to perform any preparatory act to or to further the commission of an offence under the Act.

3 See *Webster's New Millennium Dictionary of English* (Preview Edition (v.0.9.6)), available at: http://dictionary.reference.com/browse/phishing.

4 For example, the latest report from the Anti-Phishing Working Group ('APWG'), a global pan-industrial and law enforcement association set up to combat all forms of cyber fraud and identity theft, shows that conventional phishing attacks continue to escalate while other methods of fraud and theft generally show an upward trend as well. See the report at the APWG web site at: http://www.antiphishing.org/reports/apwg_report_May2006.pdf.

5 In mid-2006, there have also been reported incidents of foreign objects attached to the card reader of Automatic-Teller Machines ('ATM's) and surveillance cameras installed on those machines that are used to steal data from bank customers using them in order to steal their account information and thereby facilitate the transfer of the funds in their accounts to the scammers'.

6 Section 7, which makes it an offence to disclose access code without proper authority, does not appear applicable here as it neither involves fraud or theft nor punishes the recipient. Section 7 on unauthorised obstruction of computer usage also does not appear applicable to this subject matter. Section 9 provides for enhanced punishment for offences under ss 3, 5 and 6 of it involves 'protected computers'.

7 Under the theory of criminal justice, a component of the philosophy of law, the utilitarian reasons for punishment include deterrence, incapacitation (prevention), rehabilitation and restoration as well as retribution.

8 See The Model Data Protection Code for the Private Sector ('Model Code'). The Report on the Model Code is available at: http://www.agc.gov.sg/publications/docs/Model_Data_Protection_Code_Feb_2002.pdf.

9 But it is to be noted that there are specific provisions for the protection of certain information in some legislation, such as those relating to banking and financial information.

10 As noted, s 7 merely makes it an offence for the discloser to disclose access code without proper authority to the recipient. The recipient is likely the one that will keep or use the information for other unlawful/illegal purposes.

11 On the other hand, the positive features of the provision are that, first, it is an offence in itself without requiring the successful completion of the primary offence intended to be committed; and second, the current

punishments under sub-s (3) appear sufficiently strong. On the former, see also s 10 which makes it an offence to abet, attempt or act in preparation to or in furtherance of the commission of the offence in question under the CMA.

12 A person cheats 'by deceiving any person, [and] fraudulently or dishonestly induces the person so deceived to deliver any property to any person, or to consent that any person shall retain any property, or intentionally induces the person so deceived to do or omit to do anything which he would not do or omit if he were not so deceived, and which act or omission causes or is likely to cause damage or harm to that person in body, mind, reputation or property.' There is no general interpretation of 'property' under the Interpretation Act (Cap 1). However, it is likely that it applies to financial assets, whether represented in digital or physical form.

13 Section 22 of the Penal Code (Cap 224) provides that 'movable property' is intended to include 'corporeal property of every description, except land and things attached to the earth, or permanently fastened to anything which is attached to the earth'. The ordinary meaning of 'corporeal' is that which relates to, or has the characteristic of a material or tangible form.

14 Ibid. See the APWG report.

15 Section 11 of the CMA states that its provisions 'have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore [and that where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore [provided that] the accused was in Singapore at the material time; or the computer, program or data was in Singapore at the material time.' Similarly, s 10(2) states for that an offence of abetment, attempt or preparation to be committed, 'it is immaterial where the act in question took place' as well (contra current reach of most Penal Code provisions).

16 After years of review, the Penal Code Amendment Bill is finally undergoing substantive updates and changes since the last major review in 1984 (minor changes were also made in 1998). See Selina Lum, 'Law to be Widened to Cover Range of Electronic Crimes', *Straits Times*, 9 November 2006 at H4. There have been expansions of existing legal provisions to cover electronically perpetrated crimes, although only a few relate specifically to the concerns pertaining to cyber forgery, fraud and identity theft that are referred to in this article. For example, the amendment of s 415 on cheating extends that offence to cover cases where the deception was not the sole or main inducement for the actions relating to the property concerned. It also covers damage or harm to 'any person' (ie secondary targets) and not only the person deceived (ie primary targets). It remains to be seen whether further changes will be made to the Penal Code Amendment Bill (after the public consultation exercise conducted at: http://www.reach.gov.sg/olcp/asp/ocp/ocp01d1.asp?id=3683) or other criminal law statutes to deal more specifically and comprehensively with these and other high-technology offences.